UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/692,261	10/23/2003	Jon Cargille	MS1-1781US	1559

22801 7590 11/16/2007
LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
HA, LEYNNA A	
ART UNIT	PAPER NUMBER
2135	
MAIL DATE	DELIVERY MODE
11/16/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/692,261	**Applicant(s)** CARGILLE ET AL.	
	Examiner LEYNNA T. HA	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 September 2007*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-33* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *9/4/07*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-33 remains pending.

2. The rejection under 35 U.S.C. 101 is withdrawn.

3. The rejection under 35 U.S.C. 112, 2nd paragraph is withdrawn.

Response to Arguments

4. Applicant's arguments filed 9/4/07 have been fully considered but they are not persuasive.

Examiner traverses the argument on pg.17 for independent claim 1 pg.23 for independent claims 29. Jensworth discloses performing security checks at the operating system level and user performs tasks by accessing the system's resources or objects via processes (col.4, lines 34-35 and 42-50). The object as a kernel level security descriptor (col.5, lines 3-8). Thus, Jensworth reads on the claimed security descriptor applied to at least the kernel objects to identify at least one user. Jensworth discusses user based access token that includes a security identifier (security ID or SID) based on the user's credentials. The token also includes a privileges field listing any privileges assigned to the user (col.4, lines 55-60 and col.5, lines 10-15). Therefore, Jensworth reads on the claimed to identify a right indicating that the identified user is permitted or prohibited to perform the operation. Further, Jensworth discloses adding restricted security IDs are numbers representing processes, resource operations and the like (col.7, lines 33-35). Thus, reads on the claimed to identify one of the operations of the transaction that may be performed on the kernel object to which the security descriptor is applied. All dependent claims 2-6 and 30-33 are also rejected by virtue of their dependency.

Examiner traverses the argument on pg.20 for independent claims 7 and on pg.22 for independent claims 21, that Jensworth does not teach or show the claimed performing an operations for the transaction on the at least one kernel object in accordance with the rights accorded by the security descriptor attached to the at least one kernel object. Jensworth discusses user based access token that includes a security identifier (security ID or SID) based on the user's credentials. The token also includes a privileges field listing any privileges assigned to the user (col.4, lines 55-60 and col.5, lines 10-15). Therefore, Jensworth reads on the claimed to identify a right indicating that the identified user is permitted or prohibited to perform the operation. Further, Jensworth discloses adding restricted security IDs are numbers representing processes, resource operations and the like (col.7, lines 33-35). Thus, reads on the claimed performing an operations for the transaction on the at least one kernel object in accordance with the rights accorded by the security descriptor attached to the at least one kernel object. All dependent claims 8-14 and 22-28 are also rejected by virtue of their dependency.

Examiner traverses the argument on pg.21 for independent claims 15 and 19, that Jensworth does not teach or show the claimed identifying an operation capable of being performed on the kernel object and does not teach applies a security descriptor to at least one of the kernel objects participating in the transaction. Jensworth discusses the security descriptor also includes a system ACL or SACL which comprises entries of type audit corresponding to client actions that are to be audited. Flags in each entry indicate whether the audit is monitoring successful or failed operations, and a bitmask in the entry indicates the type or operations to be audited (col.5, lines 34-52). Jensworth discloses adding restricted security IDs are numbers representing processes, resource operations and the like (col.7, lines 33-35). Thus, reads on the claimed as recited in claims 15 and 19. All dependent claims 16-18 and 20 are also rejected by virtue of their dependency.

Claim Objections

5. Claim 20 is objected to because of the following informalities: line 2 recites "wherein" twice. Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1-33 are rejected under 35 U.S.C. 102(b) as being anticipated by Jensenworth, et al. (US 6,279,111).

As per claim 1:

Jensenworth disclose a kernel-level transaction system, comprising:

a memory; **(col.3, lines 16-23)**

one or more processors operatively coupled to the memory; **(col.2, lines 66-67 and col.3, lines 5-12)**

plural kernel objects to implement a transaction having plural operations; and **(col.2, line 66 – col.3, line 3 and col.12, lines 26-32)**

a security descriptor, applied to at least one of the kernel objects **(col.1, lines 63-65 and col.5, lines 4-8)**, to identify at least one user **(col.4, lines 53-65)**, to identify one of the operations of the transaction that may be performed on the kernel object to which the security descriptor is applied **(col.4, line 67 – col.5, line 2)**, and to identify a right indicating that the identified user is permitted or prohibited **(col.6, lines 36-67 and col.7, lines 60-67)** to perform the operation. **(col.5, lines 10-15 and 50-52 and col.11, lines 10-22)**

As per claim 2: see col.3, lines 1-3 and col.5, lines 1-4 and 30-33 and col.11,lines 25-27; discussing a system according to Claim 1, wherein the plural kernel objects include: a transaction object to represent a transaction; a resource manager object to represent a resource participating in the transaction; and an enlistment object to enlist participants in the transaction.

As per claim 3: see col.5, lines 9-15; discussing a system according to Claim 1, wherein the security descriptor comprises at least one access control entry (ACE), which includes a security identifier (SID) and rights corresponding to the SID.

As per claim 4: see col.8, lines 47-50 and col.14, lines 2-5; discussing a system according to Claim 2, wherein the security descriptor is applied to the transaction object, and the operation identified by the security descriptor includes at least one of: set information regarding the transaction object, enlist the transaction object in the transaction, render data updates in connection with the transaction object durable, abort the operation on the transaction object, transmit data from the transaction object to another object, save the current point of the transaction at the transaction object, and transmit data regarding the transaction to another device.

As per claim 5: see col.5, lines 3-20 and 45-49 and col.11, lines 25-26 and 48-49; discussing a system according to Claim 2, wherein the security descriptor is applied to the resource manager object, and the operation identified by the security descriptor includes at least one of: retrieve information regarding the resource manager object, set information regarding the resource manager object, determine the state of a transaction at a moment of transaction failure, enlist the resource manager object in a transaction, register the resource manager object in the transaction, receive notification upon resolution of a transaction at the resource manager object, and set resource data in accordance with the transaction resolution.

As per claim 6: see col.3, lines 1-3 and col.5, lines 1-4 and 30-33 and col.11,lines 25-27; discussing a system according to Claim 2, wherein the security descriptor is applied to the enlistment object, and the operation identified by the security descriptor includes at least one of: get information regarding the enlistment object, set information regarding the enlistment object, determine a state of enlistments at a moment of transaction failure obtain and reference an enlistment key, rollback the transaction and to respond to notifications, and perform operations a superior transaction manager would perform.

As per claim 7:

Jensenworth discloses a method of implementing a kernel-level transaction, comprising:

attaching a security descriptor **(col.5, lines 4-8)** to at least one of plural kernel objects **(col.2, line 66 – col.3, line 3 and col.12, lines 26-32)** utilized in a transaction; and **(col.4, line 67 – col.5, line 2)**

performing an operation for a transaction on the at least one kernel object in accordance with the rights **(col.6, lines 36-67 and col.7, lines 60-67)** accorded by the security descriptor attached to the at least one kernel object. **(col.5, lines 10-15 and 50-52 and col.11, lines 10-22)**

As per claim 8: see col.1, lines 63-65 and col.5, lines 4-8; discussing a method according to Claim 7, wherein the security descriptor includes identification for at least one user, an operation that is able to be performed on the at least one kernel object to which the security descriptor is attached, and a right indicating that the identified user is permitted or prohibited to perform the operation.

As per claim 9: see col.6, lines 29-30 and col.12, lines 26-32; discussing a method according to Claim 8, wherein the at least one kernel object is a transaction object

As per claim 10: see col.5, lines 2-3 and col.11, lines 25-27; discussing a method according to Claim 8, wherein the at least one kernel object is a resource manager object.

As per claim 11: see col.5, lines 1-4 and 30-33 and col.6,lines 28-30; discussing a method according to Claim 8, wherein the at least one kernel object is an enlistment object.

As per claim 12: see col.3, lines 1-3 and col.5, lines 1-4 and 30-33 and col.11,lines 25-27; discussing a method according to Claim 9, wherein the operation identified by the security descriptor attached to the transaction object includes at least one of: set information regarding the transaction object, enlist the transaction object in the transaction, render data updates in connection with the transaction object durable, abort the operation on the transaction object, transmit data from the transaction object to another object, save the current point of the transaction at the transaction object, and transmit data regarding the transaction to another device.

As per claim 13: see col.5, lines 3-20 and 45-49 and col.11, lines 25-26 and 48-49; discussing a method according to Claim 10, wherein the operation identified by the security descriptor attached to the resource manager object includes at least one of: retrieve information regarding the resource manager object, set information regarding the resource manager object, determine the state of a transaction at a moment of transaction failure, object, and enlist the resource manager object in a transaction, register the resource manager object in the transaction, receive notification upon resolution of a transaction at the resource manager set resource data in accordance with the transaction resolution.

As per claim 14: see col.5, lines 3-20 and 45-49 and col.11, lines 10-22; discussing a method according to Claim 11, wherein the operation identified by the security descriptor includes at least one of: get information regarding the enlistment object, set information regarding the enlistment object, determine a state of enlistments at a moment of transaction failure, obtain and reference an enlistment key, rollback the transaction and to respond to notifications, and perform operations a superior transaction manager would perform.

As per claim 15:

Jensenworth discloses a computer-readable medium having stored thereon an object attached to a kernel object, the object comprising:

a first data entry identifying at least one user; **(col.2, lines 2-4)**

a second data entry identifying an operation **(col.7, lines 33-40)** capable of being performed on the kernel object **(col.1, lines 63-65 and col.5, lines 4-8)** by the user identified by the first data entry; and **(col.3, lines 54-55 and col.4, lines 48-57)**

a third data entry indicating a right for the user **(col.6, lines 36-67 and col.7, lines 60-67)** identified by the first data entry to perform the operation identified by the second data entry. **(col.5, lines 10-15 and 50-52 and col.11, lines 10-22)**

As per claim 16: see col.8, lines 47-50 and col.14, lines 2-5; discussing a computer-readable medium according to Claim 15, wherein the kernel object is a transaction object, and the identified operation includes at least one of: set information regarding the transaction object, enlist the transaction object in the transaction, render data updates in connection with the transaction object durable, abort the operation on the transaction object, transmit data from the transaction object to another object, save the current point of the transaction at the transaction object, and transmit data regarding the transaction to another device.

As per claim 17: see col.5, lines 3-20 and 45-49 and col.11, lines 10-22; discussing a computer-readable medium according to Claim 15, wherein the kernel object is a resource manager object, and the identified operation includes at least one of: retrieve information regarding the resource manager object, set information regarding the resource manager object, determine the state of a transaction at a moment of transaction failure, enlist the resource manager object in a transaction, register the resource manager object in the transaction, receive notification upon resolution of a transaction at the resource manager object, and set resource data in accordance with the transaction resolution.

As per claim 18: see col.5, lines 3-20 and 45-49 and col.11, lines 25-26; discussing a computer-readable medium according to Claim 15, wherein the kernel object is an enlistment object, and the identified operation includes at least one of: get information regarding the enlistment object, set information regarding the enlistment object, determine a state of enlistments at a moment of transaction failure, obtain and reference an enlistment key, rollback the transaction and to respond to notifications, and perform operations a superior transaction manager would perform.

As per claim 19:

Jensenworth discloses a transaction method, comprising:

implementing a transaction among kernel objects; and **(col.2, line 66 – col.3, line 3 and col.12, lines 26-32)** securing the transaction utilizing an operating system security model **(col.4, lines 31-45 and col.13, lines 61-64)** that applies a security descriptor to at least one of the kernel objects participating in the transaction. **(col.6, lines 36-67 and col.7, lines 60-67)**

As per claim 20: see col.4, lines 31-45 and col.13, lines 61-64; discussing a transaction method according to Claim 19, wherein wherein the security descriptor identifies at least one user, an operation to be performed on the at least one kernel object to which the security descriptor is applied, and a right indicating that the identified user is permitted or prohibited to perform the operation.

As per claim 21:.

Jensenworth discloses a method of implementing a transaction, comprising:

attaching a security descriptor **(col.1, lines 63-65 and col.5, lines 4-8)** to at least one of plural objects utilized in a transaction; and **(col.2, line 66 – col.3, line 3 and col.12, lines 26-32)**

performing an operation for a transaction on the at least one object in accordance with the rights **(col.6, lines 36-67 and col.7, lines 60-67)** accorded by the security descriptor attached to the at least one object. **(col.5, lines 10-15 and 50-52 and col.11, lines 10-22)**

As per claim 22: see col.5, lines 4-8 and col.7, lines 25-40; discussing a method according to Claim 21, wherein the security descriptor includes identification for at least one user, an operation to be performed on the at least one object to which the security descriptor is attached, and a right indicating that the identified user is permitted or prohibited to perform the operation.

As per claim 23: see col.2, line 66 – col.3, line 3 and col.12, lines 26-32; discussing a method according to Claim 22, wherein the at least one object is a transaction object.

As per claim 24: see col.5, lines 2-3 and col.11, lines 25-27; discussing a method according to Claim 22, wherein the at least one object is a resource manager object.

As per claim 25: see col.5, lines 9-12 and col.6, lines 28-30; discussing a method according to Claim 22, wherein the at least one object is an enlistment object.

As per claim 26: see col.5, lines 10-15 and 50-52 and col.11, lines 10-22; discussing a method according to Claim 23, wherein the operation identified by the security descriptor attached to the transaction object includes at least one of: set information regarding the transaction object, enlist the transaction object in the transaction, render data updates in connection with the transaction object durable, abort the operation on the transaction object, transmit data from the transaction object to another object, save the current point of the transaction at the transaction object, and transmit data regarding the transaction to another device.

As per claim 27: see col.5, lines 3-20 and 45-49 and col.11, lines 10-22; discussing a method according to Claim 24, wherein the operation identified by the security descriptor attached to the resource manager object includes at least one of: retrieve information regarding the resource manager object, set information regarding the resource manager object, determine the state of a transaction at a moment of transaction failure, enlist the resource manager object in a transaction, register the resource manager object in the transaction, receive notification upon resolution of a transaction at the resource manager object, and

set resource data in accordance with the transaction resolution.

As per claim 28: see col.5, lines 10-15 and 50-52 and col.11, lines 10-22; discussing a method according to Claim 25, wherein the operation identified by the security descriptor includes at least one of: get information regarding the enlistment object, set information regarding the enlistment object, determine a state of enlistments at a moment of transaction failure, obtain and reference an enlistment key, rollback the transaction and to respond to notifications, and perform operations a superior transaction manager would perform.

As per claim 29:

Jensenworth discloses a kernel-level transaction system, comprising:

<u>a memory;</u> **(col.3, lines 16-23)**

<u>one or more processors operatively coupled to the memory;</u> **(col.2, lines 66-67 and col.3, lines 5-12)**

means for implementing a transaction among kernel objects; and **(col.2, line 66 – col.3, line 3 and col.12, lines 26-32)**

means for securing the transaction by applying a security descriptor to at least one of the kernel objects **(col.1, lines 63-65 and col.5, lines 4-8)**, wherein the security descriptor identifies at least one user **(col.7, lines 33-40)**, an operation to be performed on the kernel object to which the security descriptor is applied, and a right **(col.6, lines 36-67 and col.7, lines 60-67)** indicating that the identified user is permitted or prohibited to perform the operation. **(col.5, lines 10-15 and 50-52 and col.11, lines 10-**

22)

As per claim 30: see col.5, lines 2-3 and col.11, lines 25-27; discussing a system according to Claim 29, wherein the kernel objects include: a transaction object to represent a transaction; a resource manager object to represent a resource participating in the transaction; and an enlistment object to enlist participants in the transaction.

As per claim 31: see col.5, lines 10-15 and 50-52 and col.11, lines 10-22; discussing a system according to Claim 30, wherein the security descriptor is applied to the transaction object, and the operation identified by the security descriptor includes at least one of: set information regarding the transaction object, enlist the transaction object in the transaction, render data updates in connection with the transaction object durable, abort the operation on the transaction object, transmit data from the transaction object to another object, save the current point of the transaction at the transaction object, and transmit data regarding the transaction to another device.

As per claim 32: see col.5, lines 10-15 and 50-52 and col.11, lines 10-26; discussing a system according to Claim 30, wherein the security descriptor is applied to the resource manager object, and the operation identified by the security descriptor includes at least one of: retrieve information regarding the resource manager object, set information regarding the resource manager object, determine the state of a transaction at a moment of transaction failure, enlist the resource manager object in a transaction, register the resource manager object in the transaction, receive notification upon resolution of a transaction at the resource manager object, and set resource data in accordance with the transaction resolution.

As per claim 33: see col.5, lines 34-38 and col.11, lines 10-22; discussing a system according to Claim 30, wherein the security descriptor is applied to the enlistment object, and the operation identified by the security descriptor includes at least one of: get information regarding the enlistment object, set information regarding the enlistment object, and determine a state of enlistments at a moment of transaction failure.

Conclusion

7. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LHa

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100